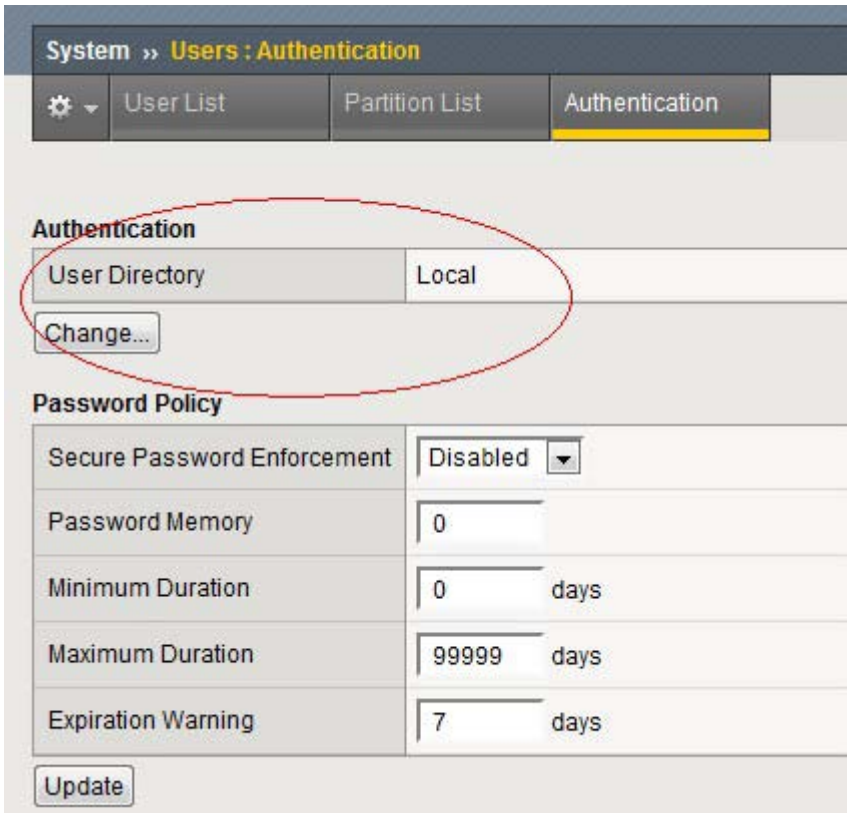
F5 设备管理帐号远程认证、授权之 Radius 版

V10.1 在管理帐号的集中统一验证授权方面有了很大的提高，本文介绍如何实现基于 radius 进行管理帐号认证及授权。

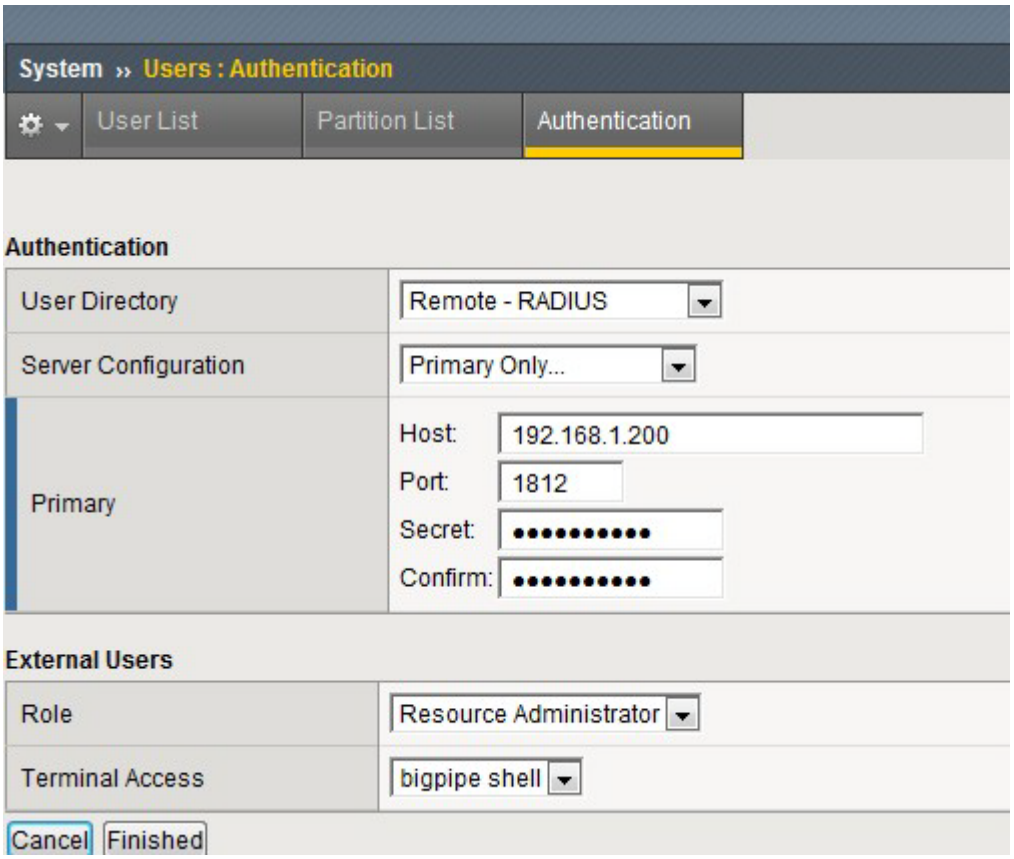
原理：
当用户登录时 F5 能够与 radius 服务器进行通信，得到 radius 对身份验证的结果（通过或不通过 失败等）。
如果身份验证失败，拒绝登陆，并在/var/log/secure,/var/log/aduit 日志文件中记录失败信息
如果身份验证通过，则利用 radius 服务器返回的属性在本地查找对应匹配的 remoterole，根据 remoterole 中的定义赋予用户 console/user partition 以及对应的 role（即系统内置的 guest,operator,manager 等内置的 role 权限），同时记录相关日志
如果身份验证通过，但无法找到匹配的 remoterole，那么使用配置 radius 时候所指定的“External Users”设置赋权---系统默认为 no access，即默认情况下即使验证通过也禁止访问。

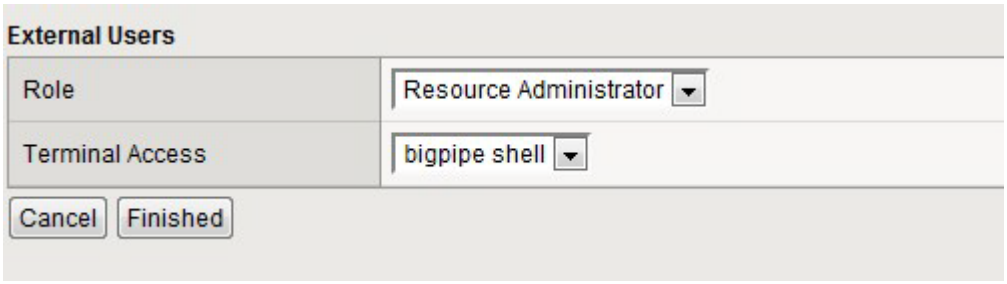
设置方法：
一、F5 部分设置

1. 点击 system-users 菜单进入下图，并点击 change，将验证位置改为 remote-radius



2.随后将出现如下界面：





解释：

Server 处填写 radius 服务器服务 IP，如有多台则都填入，注意 F5 使用管理口 IP 与验证服务器通信

Secret 是用来加密密码的 key，与 radius 服务器端设置的 key 相同

External users 部分配置缺省外部用户所用的 role 及 shell 的级别。注意不同版本的这部分关于 shell 的选项不同。10.0 的版本不支持配置 tmsh 在这里，10.1 即可。

3．至此，基本 F5 端配置完成，但是上述配置存在缺陷，即缺省所有外部用户都只能被赋予相同的 role，显然实际工作中肯定有很多不同 role 的用户，因此必须实现不同的用户或用户组能有不同的 role 权限，方法有两种：

A.在 F5 的 user 中添加所有外部用户的用户名，并逐一为其设置各自的 role。此方法的好处是 radius 服务器端不用考虑分组，radius 服务器等于只负责验证，不负责授权，授权由本地来进行。

B.使用 b remoterole 命令在 F5 上配置不同的用户组管理不同的 role，F5 将在 radius 服务器所返回的响应中查找是否存在匹配的 attribute，如果查到匹配则分配对应的 role

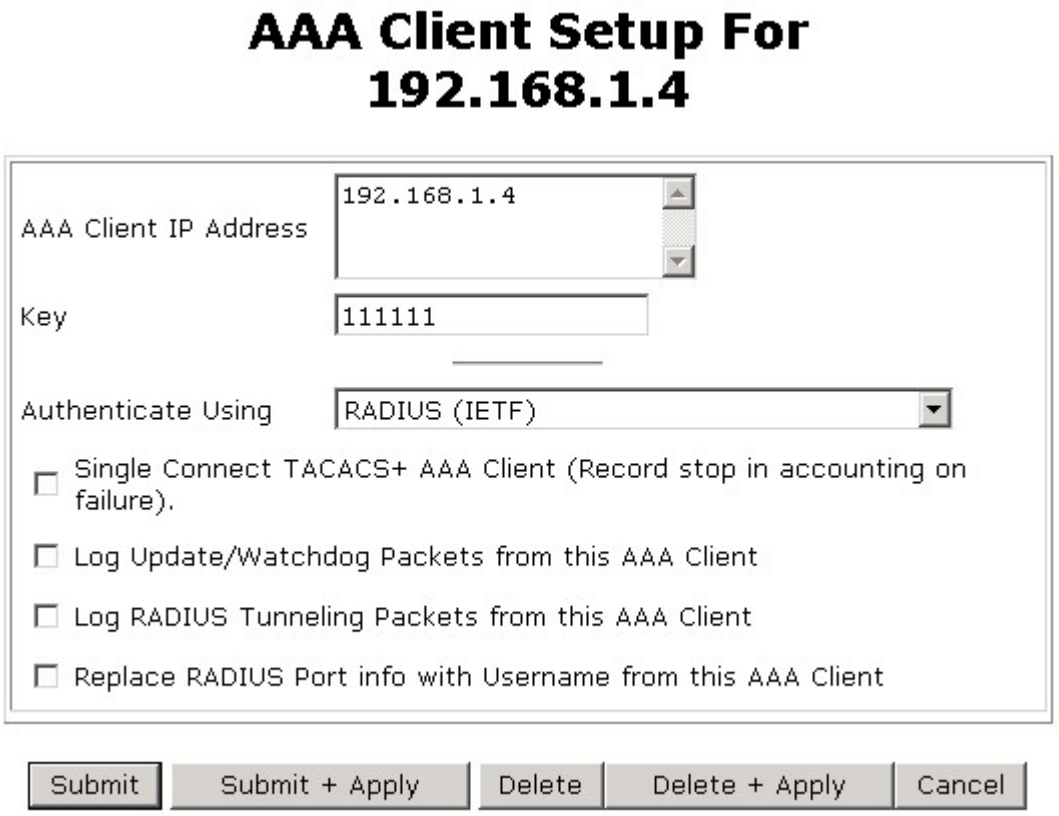
本文只讲述 B 方法。具体的 b remoterole 如何设置见下文。

二、RADIUS 服务器设置

不同的软件设置方法不同，本文以 CISCO ACS 4.0 为例。

1. Cisco acs 安装方法略
2. 检查 service.msc 确保 radius 服务已启动
3. 点击左侧 Network configuration

在 AAA clients 中添加 F5 ：

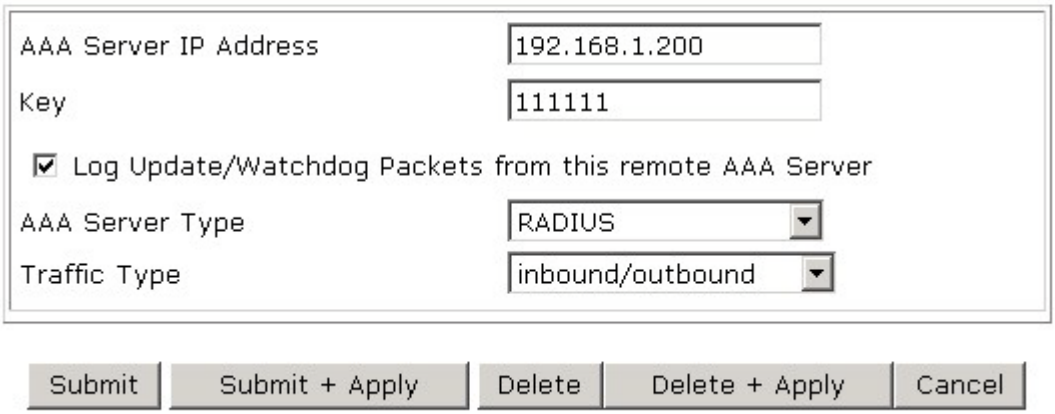


Client ip 填写 F5 管理口地址

请注意 key 部分，填写与 F5 上一致的 key。

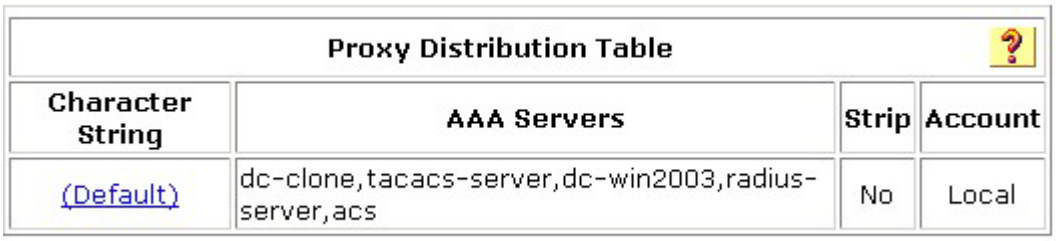
点击 submit+apply 提交后，会自动回到 network configuration 主界面，在 AAA servers 中添加一个 AAA server 定义:

AAA Server Setup For radius-server

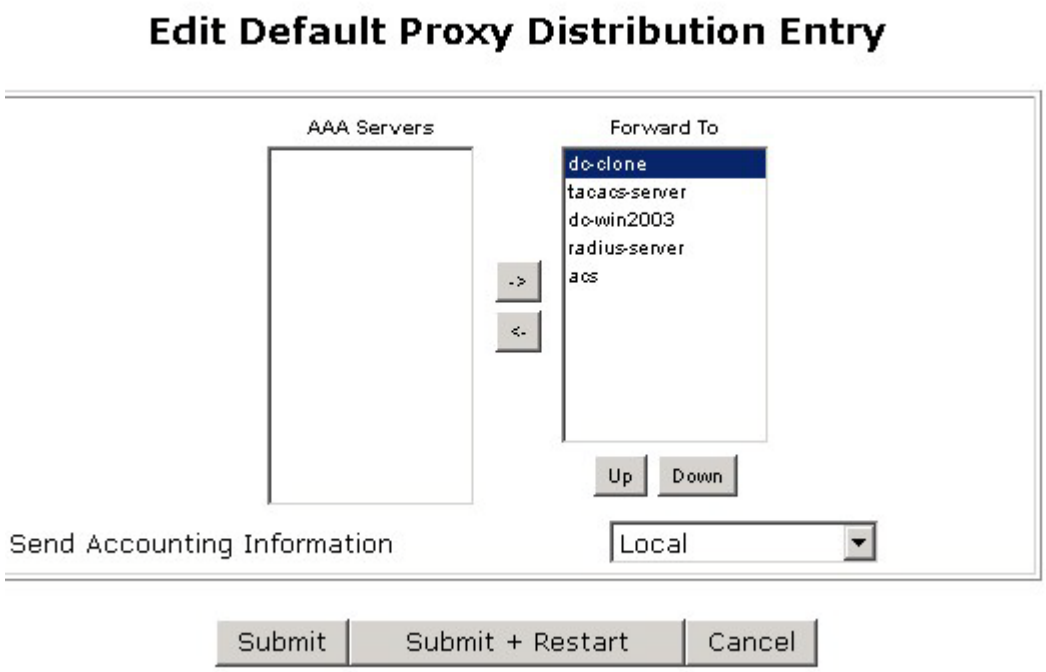


一样需要注意 KEY 部分，填写和 F5 端一致设置。
点击 submit+apply 提交。

另外，在 network configuration 中的 default proxy distribution tables 中，要把当前的所有 AAA SERVER 都选择到 forwart to 一栏中

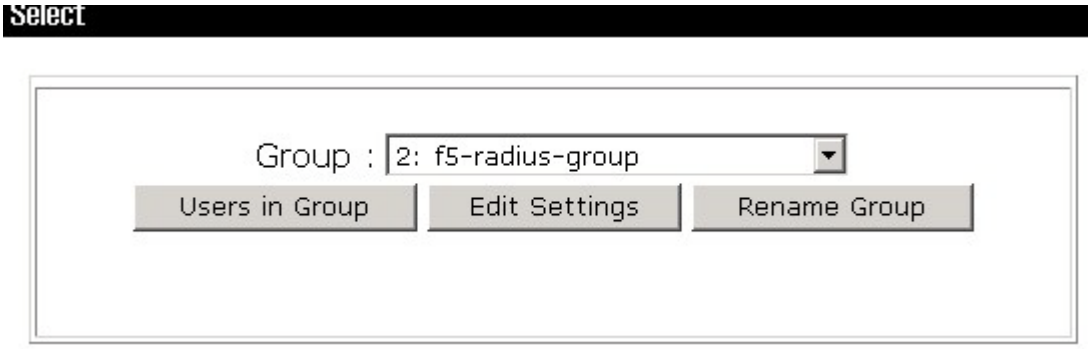


Proxy Distribution Table			
Character String	AAA Servers	Strip	Account
(Default)	dc-clone,tacacs-server,dc-win2003,radius-server,acs	No	Local

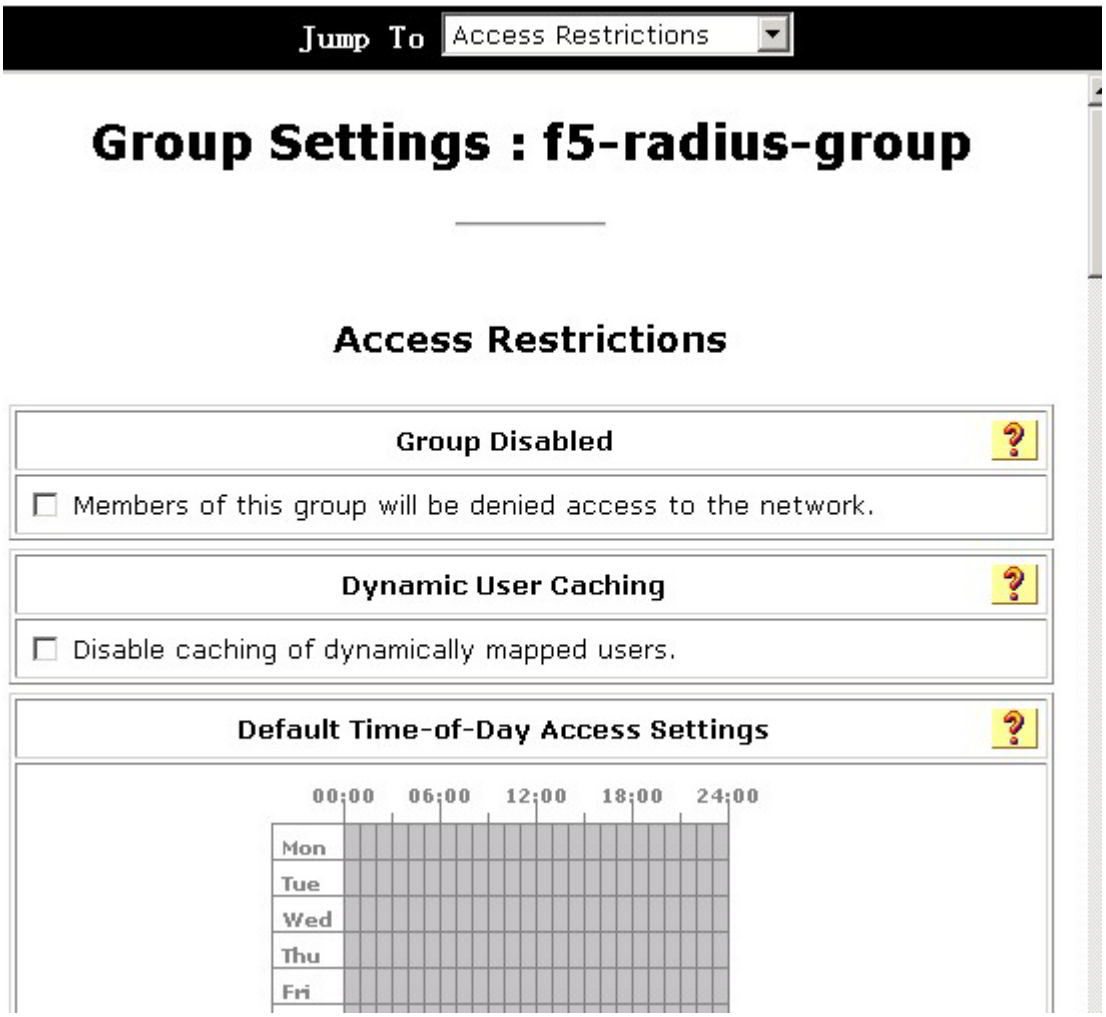


4. 设置用户组属性

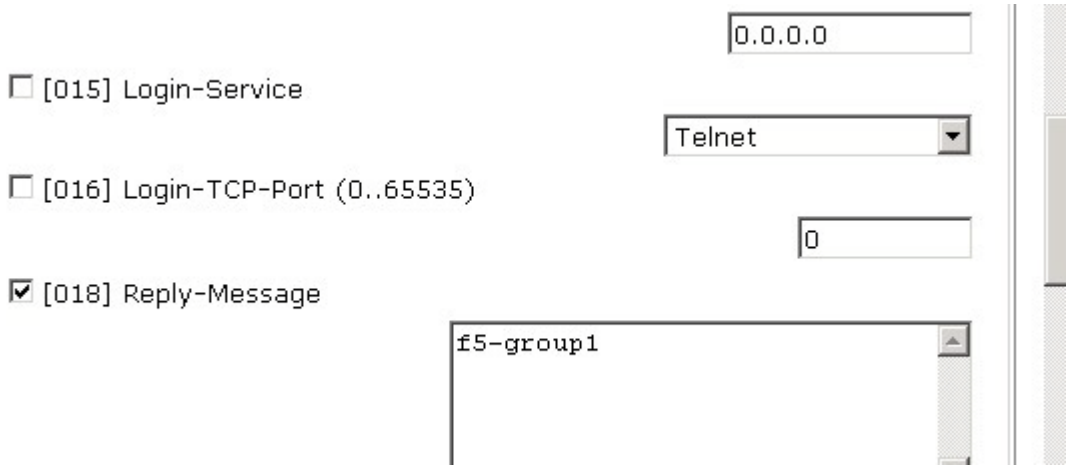
点击左侧 Group setup，任意选择一个内置的组，



注意这里的组 1 的名字已被我自定义，你可以使用缺省名.选择一个组后点编辑设置，出现下图：



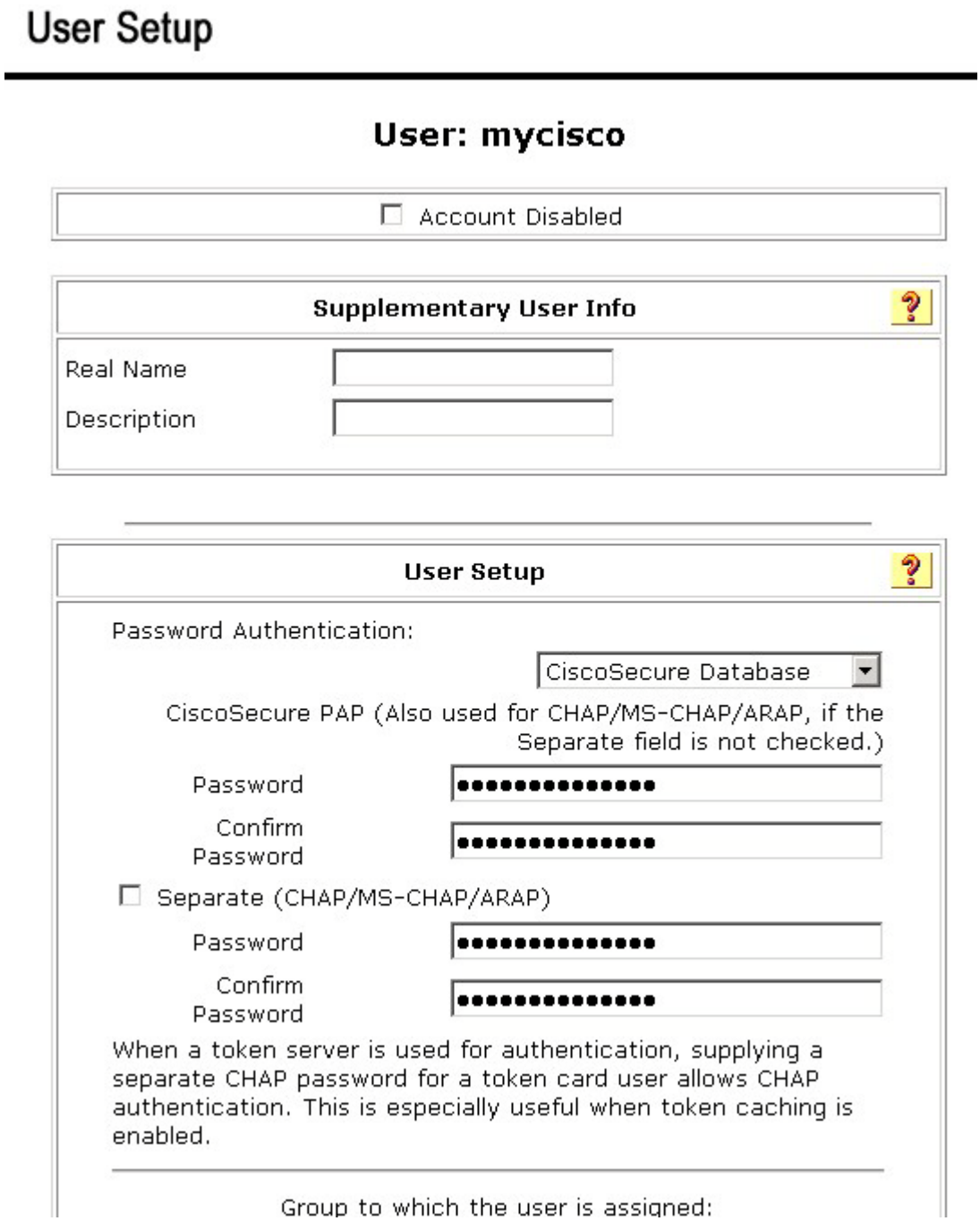
直接向下拉页面到 radius setting 部分，可以忽略其他所有设置，挑选属性 18 配置：



注意按上图设置，这里定义的就是为了让 F5 查找匹配一个 remoterole 的。
其他部分保持缺省，提交 group 设置。

6.添加用户

点击左侧 user setup ，输入一个用户名，点 add/edit:



注意不要勾选 account disabled，上图中所有密码处设置你要的密码，全部一样即可，剩余部分保持缺省，提交配置。

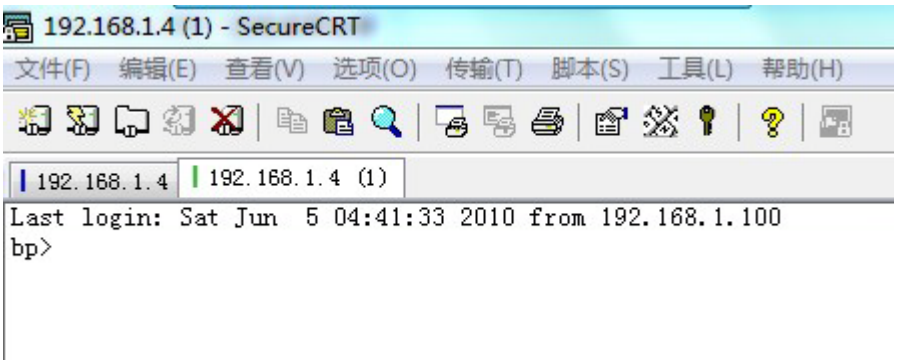
至此,ACS 部分配置完毕，开始调试。

小结：

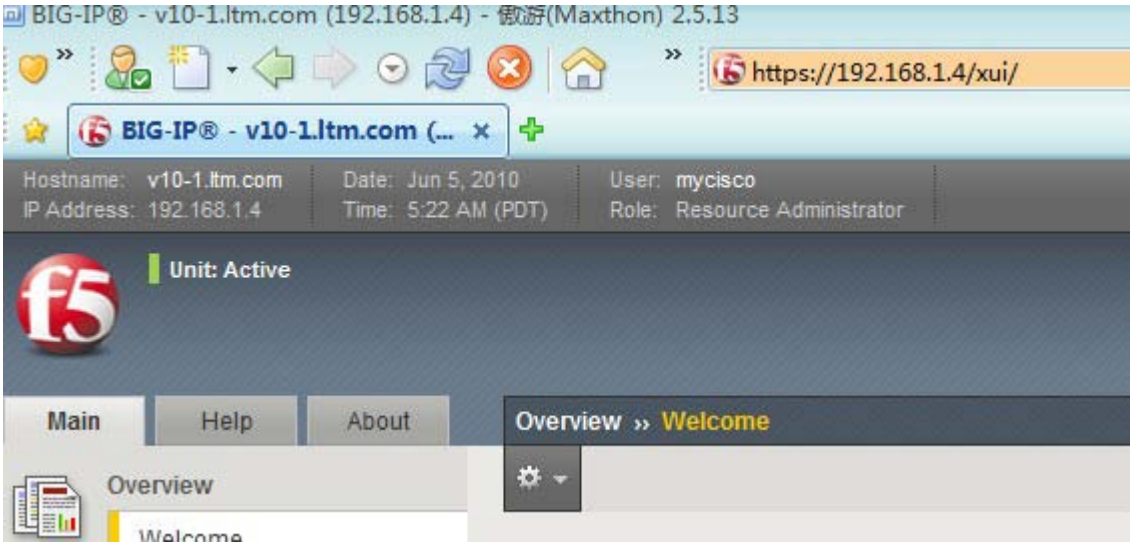
1. F5 启用了外部验证，不加密，设置了缺省的外部用户 role 及 sh 权限 （resource administrator/bigpiple shell），没有设置额外的 remoterole
2. ACS 设置不加密，配置了一个名为 mycisco 的用户，并设置了一个自定义属性

三、调试

1. 尝试使用 mycisco 帐号登录 ssh 和 web



Ssh 登录得到上述效果,符合要求，自动进入 b shell。



WEB 登录，显示 role 为 resource administrator ，符合要求。

2. 添加 remoterole 配置来 override 当前缺省的 role，在命令行中输入如下命令：

[root@v10-1:Active] config # b remoterole role info myrole2 {attribute "Reply-Message=myf5" console "enable" deny "disable" line order 2 role "administrator" user partition "all"}Myrole, 定义的 role 名字

Reply-Message=myf5 这是在 radius 中设置的自定义 attribute

Console 部分指定 shell 级别 或禁用

Line order 用来排序配置在配置文件的顺序，F5 顺序检查，查到第一个匹配即认为成功

Uer partition 指定用户管理域

命令配置完毕后，可以用 b remoterole list 显示：

```
[root@v10-1:Active] config # b remoterole list
remoterole {
    role info {
        myrole {
            attribute "f5-tacacs-group=test"
            console "tmsh"
```

```
            line order 1
            role "administrator"
            user partition "all"
        }
        myrole2 {
            attribute "Reply-Message=myf5"
            console "enable"
            deny disable
            line order 2
            role "administrator"
            user partition "all"
        }
    }
}
```

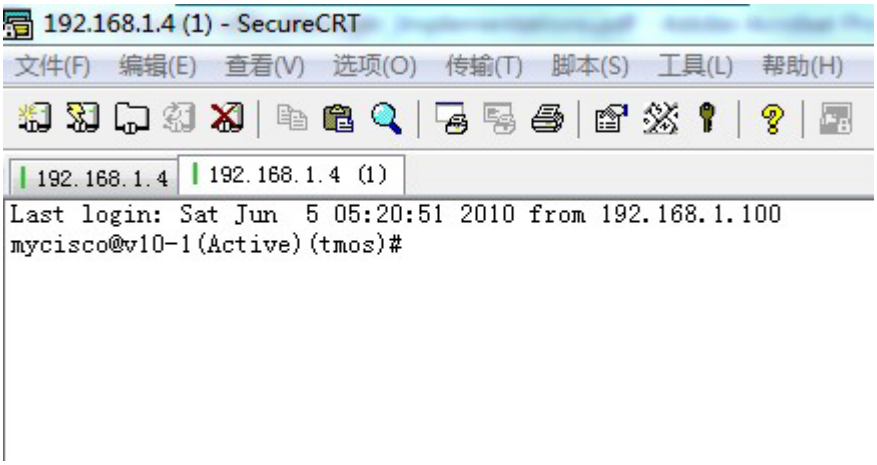
命令结构：

**bigpipe remoterole role info <user group> attribute (<string> | none) console **

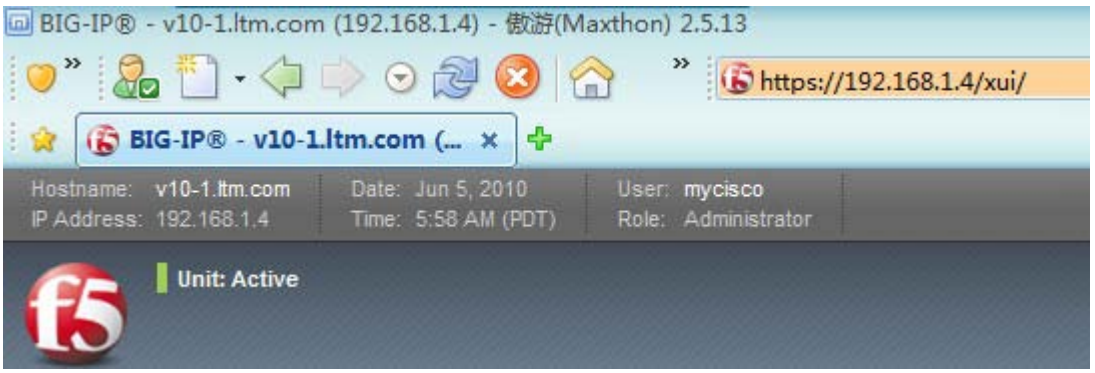
**(enable | disable) line order <number> role <user role> user partition **

(<string> | none)

3. 检查上述配置是否生效，仍然使用 mycisco 帐户登录，如果生效，此时应该拥有管理员权限及 tmsh 的权限



成功！



至此配置完成，测试成功。

附 1：
www.myf5.net 查看TACACS+版 设置方法！